AMA
AMERICAN
MEDICAL
ASSOCIATION

Michael D. Maves, MD, MBA, Executive Vice President, CEO

June 8, 2007

Michael O. Leavitt
Secretary
Office of the Secretary
U.S. Department of Health & Human Services

Daniel R. Levinson
Inspector General
Office of the Inspector General
U.S. Department of Health & Human Services

Leslie Norwalk
Acting Administrator
Centers for Medicare & Medicaid Services
U.S. Department of Health & Human Services

Re: **Health Insurance Portability and Privacy Act Administrative Simplification: National Plan and Provider Enumeration System Data Dissemination Notice**

Dear Secretary Leavitt, Inspector General Levinson, and Acting Administrator Norwalk:

On behalf of the physician and student members of the American Medical Association (AMA), we are contacting you to express the AMA's serious concerns with the May 30, 2007, National Plan and Provider Enumeration System (NPPES) Data Dissemination Notice (CMS-6060-N) (Dissemination Notice). We have three general issues that we would like to address on an expedited basis in order to avoid both the imminent irreparable harm to the privacy interests of physicians and compromising the integrity of the Medicare Trust Fund. We have summarized these concerns immediately below and followed with a more detailed discussion.

First, the Dissemination Notice provides a mere 30-day window for physicians to remove personally identifiable information that the agency indicates is "optional." If physicians do not remove the data before the deadline, it will be released by the agency to

the general public. However, the agency did not develop nor implement a plan to communicate to physicians that this information would be released to the general public before the 30-day window began. Thus, many physicians will not be able to remove the information before it is released to the public by the agency. The "optional" information includes an array of physician billing identification numbers used by public and private payers, as well as individually assigned Drug Enforcement Administration (DEA) numbers used to prescribe controlled substances. Also, when physicians supplied this information they reasonably believed that they were, in fact, required to submit the information. Furthermore, they likely concluded that the agency would only release the information for the limited purposes specified in the Privacy Act Statement attached to the National Provider Identifier (NPI) Application/Update Form—all circumstances identified involve uses to fulfill government functions and none could even remotely be characterized as a release to the general public.

Second, the Dissemination Notice does not specify the security and privacy measures or policies that will be utilized when personally identifiable information is shared with other public agencies. Equally important, the Dissemination Notice does not provide information on what steps will be taken to mitigate harm if, and when, personally identifiable information that is otherwise protected from public disclosure is compromised because of a security breach. This is a significant omission in light of Centers for Medicare & Medicaid Services' (CMS) transfer of physician personally identifiable information to the U.S. Department of Veterans Affairs (VA) and the recent, subsequent VA security breach impacting 1.3 million physicians and other health care professionals. The response of the VA and CMS to the breach exacerbated and increased the risk of identity theft. Both agencies delayed for months before informing affected physicians about the breach.

Third, the Dissemination Notice does not specify the legal rationale, standard(s), or analysis utilized by the agency to support the release of a substantial amount of personally identifiable physician information to the general public (as opposed to a limited amount to only those individuals with a legitimate purpose). Broad assertions that the agency is compelled to release personally identifiable physician information that, without question, will help facilitate widespread identity theft and quite possibly fraud on the Medicare program are unavailing. This is particularly true given that such information has been treated as protected pursuant to the Privacy Act and Freedom of Information Act (FOIA) exemption(s) previously by the agency. Note that some of the very same data that the VA has compromised in its massive security breach are substantially the same information that CMS now indicates it will make readily available to any member of the public with access to a computer. This, obviously, begs the question as to what legal standards compel two substantially different conclusions as to whether it is legally permissible to publicly disclose the same personally identifiable information.

As a result of the foregoing, we have the following recommendations—the majority of which we submitted previously to the agency. CMS should revise and issue the Dissemination Notice consistent with the following provisions:

1. **The agency should immediately remove all "optional" information from the database.**
2. **Any information that CMS characterizes as "optional" should <u>never</u> be released to the general public since it will increase identity theft and help facilitate the activities of those intent on defrauding Medicare, Medicaid, and private payers.**
3. **The remainder of the information in the database that CMS has indicated will be released to the public 30 days after the Dissemination Notice was issued in the Federal Register, should not be released until the issues raised in this letter have been addressed.**
4. **Limit access to the information specified below to only those with a legitimate need for the NPIs (i.e., HIPAA covered entities and their business associates).**
5. **Release of information associated with the NPI number should be kept to a minimum; any public-availability should be no more extensive than what is available through the Unique Physician Identification Number (UPIN) look-up directory.**
6. **A physician's home address should never be released.**
7. **NPI numbers should not be sold.**
8. **Continue assigning UPINs[1] and maintaining the Medicare UPIN Registry as well as the Registry "look up functionality" through the entire CMS NPI contingency timeframe.**

As detailed at greater length below, the course that CMS has elected to pursue places physician privacy interests at significant risk and poses a substantial threat to the program integrity of Medicare and Medicaid. The AMA does not believe that this policy decision was hastily developed—issuance of the Dissemination Notice is nearly a year and a half over due. However, the policies contained in the Dissemination Notice are ill-advised and the implementation unduly rushed, and will, undoubtedly, subject physicians to a heightened risk of identity theft. We cannot overstate the gravity with which we view this situation.

Background

As you are well aware, the NPPES Data Dissemination policy is of great importance to physicians and the rest of the health care industry. The Dissemination Notice is supposed to specify who will have access to the NPI numbers, what information associated with each number will be available to the public, and how the NPI numbers and data can be accessed. In the interest of safeguarding the privacy and security of personally identifiable physician information, as well as Medicare and Medicaid program integrity, the AMA has sent several

[1] We were informed that CMS will discontinue assigning UPINS on June 29, 2007, and will disable the CMS UPIN Registry and its "look up" functionality on September 30, 2007.

letters to CMS that include recommendations concerning access to physicians' NPI numbers and how the data submitted by physicians to obtain a NPI number should be protected. On several occasions the AMA has urged the agency to limit access to the NPI numbers to only those individuals and entities with a legitimate purpose in accessing the NPI numbers, including other physicians, health care providers, HIPAA covered entities, and their business associates. Limiting access to only appropriate individuals and entities will reduce the risk of identity theft. It will also minimize the ability of individuals intent on defrauding the Medicare and Medicaid programs from obtaining NPI numbers and other personally identifiable physician information through "one-stop shopping" in order to perpetrate criminal acts.

Despite all of the foregoing, the Dissemination Notice provides that the NPI numbers and the majority of the associated data elements will be made available to the public through a "query-only" online database as well as a downloadable file. These online queries would be difficult to trace to any particular individual; thereby, increasing the ability of individuals intent on defrauding the Medicare program or perpetrating other criminal acts, such as identity theft, to access this financial information with minimal chance of detection. Entities and individuals may also request from CMS the data in special formats not supported by the database.

The Notice is Confusing and Inaccurate & 30-Day Window to Remove "Optional" Data is Unreasonable

The Dissemination Notice has significant substantive shortcomings. It does not accurately nor clearly specify the data that the agency will release to the general public, nor does it provide a reasonable amount of time for physicians to remove "optional" personally identifiable information that could be used by others to defraud the Medicare program and/or perpetrate identity theft.

CMS delayed issuing the Dissemination Notice for over a year-and-a-half and will only allow physicians 30 days to remove any information supplied on the NPI Application/Update Form that was identified as "optional." This is neither reasonable nor rational. The 30-day window to remove information (with limited or no actual notice to physicians that this option is available) subjects hundreds of thousands of physicians to the very real risk of identity theft primarily because the agency will not provide adequate time or outreach to notify physicians that it is permissible to remove this information in order to avoid wide spread public disclosure. According to CMS, the "optional" information at issue could include DEA numbers, email addresses, unique insurance billing numbers assigned to physicians, and Medicaid billing numbers. CMS staff indicated that an outreach plan had not been developed to inform physicians of this option and the 30-day deadline at the time that the Dissemination Notice was issued. Thirty days is not an adequate amount of time to notify physicians when the clock has already started and CMS has no outreach plan in place. Furthermore, it does not account for the fact that physicians will need time to remove the "optional" information. The foregoing is particularly true for physicians requesting changes

via paper. The lack of an outreach plan and an insufficient amount of time to provide notice will prevent physicians from exercising their option to remove the information before it is released.

The release of the "optional" information is *truly unacceptable* given that there is a real question as to whether physicians understood such information was "optional" based on a number of factors including the manner in which CMS designed the NPI Application/Update Form.[2] Also, physicians had every reason to believe the "optional" information (as well as all the other personally identifiable information) would not be disclosed in light of the assurances contained on the Privacy Act Statement attached to the NPI Application. It is very important to underscore the point that many physicians supplied information on the NPI Application/Update Form well in advance of CMS issuing the Dissemination Notice since they were required to have a NPI number before the Dissemination Notice was even issued.

Throughout the NPI application and Medicare enrollment application, two processes which are closely linked, CMS repeatedly warns physicians that failure to fully and completely answer all of the questions on these forms will result in processing delays and in some cases outright denials. This is not a hollow warning given that CMS has substantial backlogs in processing enrollments that span upwards of 6 months in some regions of the country. This has financial consequences for physicians—particularly those entering the program for the first time who will not receive payment until the processing is completed. Further, CMS included the statement below on the NPI Application/Update Form in <u>three separate locations</u> including at the top of the Application in bold, in the Privacy Statement, and at the top of the Instructions Form:

> Failure to provide complete and accurate information may cause your application to be returned and delay processing of your application. In addition, you may experience problems being recognized by insurers if the records in their systems do not match the information you have furnished on this form.

The fact that CMS included this warning repeatedly on the application would reasonably lead a physician to believe that if any of the fields were left "incomplete" including the "optional" fields that the processing of the application would be "returned or delayed." Also, the actual application does not identify the "optional" data elements. Instead CMS buried the identification of "optional" elements on the Instructions Form in fine print. In addition, the Privacy Act Statement attached to the NPI Application/Update Form was drafted in a manner that clearly leads physicians (and any other lay person) to believe that the information that they were submitting on the application would be used solely "to assign a unique health identifier . . . for use on standard transactions." The agency reassured physicians on this Privacy Act Statement that "individually identifiable providers' data are

[2] We understand CMS is moving ahead with changes to the NPI application form. It remains unclear how these changes will impact the "required" versus "optional" data elements nor are the impact of these changes discussed in the Dissemination Notice.

protected by the Privacy Act of 1974." Furthermore, the Privacy Act Statement lists specific circumstance when information *may* be disclosed—all of which involve state or federal public agency functions. Not one of the specific circumstances listed by CMS even remotely could be characterized as permitting general disclosures to the public at large. Finally, the Dissemination Notice does not adequately identify the data elements that the agency will disclose and the information that the agency has concluded it is required to withhold from public disclosure. First, in the narrative portion of the Dissemination Notice, the agency states it is prohibited from disclosing physician Social Security Numbers (SSNs), Internal Revenue Service Individual Taxpayer Numbers (IRS ITINs), and dates of birth (DOB). CMS asserts that such disclosures "are not disclosable under [the Freedom of Information Act] FOIA." The data elements that the agency concluded are required to be disclosed under FOIA are listed in a matrix. However, there are data elements that CMS requires physicians to submit in the NPI Application/Update Form such as state and country of birth that CMS personnel have indicated are not subject to disclosure pursuant to FOIA. Neither of these items are referenced in the Dissemination Notice. Thus, the Dissemination Notice is substantively defective. It does not correctly identify the data elements that CMS will not disclose. **The Dissemination Notice, at a minimum, should be reissued to correct this substantive error and matrices utilized to identify the information that <u>will be disclosed</u> and that <u>will not be disclosed</u>.**

CMS should never disclose the "optional" information submitted by physicians to the general public and must clarify the Dissemination Notice to correctly identify information that is subject to widespread public disclosure. All "optional" information should be deleted by CMS since it was not necessary for CMS to meet its statutory obligations and it was provided by physicians based on misleading written agency assurances that it would be protected from disclosure. Failure to do the foregoing will help facilitate identity theft and subjects private and public payers to heightened risk of fraud and abuse.

Policies & Procedures Concerning Database Security Lacking

We are deeply concerned that CMS has not identified security measures and policies to protect the privacy of physician personally identifiable information. We expected such information would be contained in the Dissemination Notice in light of the rash of security and privacy breaches over the past several years at large private corporations and federal agencies. The Dissemination Notice did not provide *any* discussion or analysis of policies and procedures concerning interagency or intergovernmental transfers of personally identifiable physician data that should not be disclosed to the general public, for example. We believe strongly that the agency must adopt policies and procedures to protect the security of the data submitted by physicians as well as policies and procedures that govern contingency plans to mitigate damage if, and when, breaches occur. This should not be an afterthought. It should not be delegated solely or primarily to technical personnel nor treated as an incidental matter.

The lack of policy on this point in the Dissemination Notice is particularly troubling given CMS's recent role in what is likely to be the single largest unauthorized disclosure of physician personally identifiable information in history. CMS shared physician billing information with the VA under a data use agreement covering 1.3 million physicians and other health care professionals. The VA used the data to support studies concerning diabetic veterans who were eligible for both Medicare and VA benefits. The studies were to be used to develop a clear picture of public health care usage and cost patterns. The VA reported that a portable laptop with data provided by CMS "went missing" in January. The data included demographic information and identifiers, such as the Unique Physician Identifier Number (UPIN), dates of birth, state license numbers, business addresses and employer identification numbers (EIN). We were also informed that CMS supplied the VA *with more personally identifiable physician information than requested by the VA* to fulfill the goals of the data use agreement including physician Social Security numbers. Incidentally, of the identified data listed above, CMS now intends to release to the general public the NPI number as well as state licensure numbers, business addresses, and an array of other personally identifiable physician information. We are deeply dismayed that CMS has indicated that it is conducting an internal review of its own data release procedures *after the VA data breach as opposed to ensuring such measures were in place and implemented before the breach occurred*. Furthermore, CMS's forthcoming disclosure of substantially the same information that the VA was obliged to protect from public disclosure and did not, calls into question the legal validity of the Dissemination Notice.

The VA and CMS contingency policies and procedures in response to the data breach were not implemented in a manner that would mitigate the damage of the breach. While the incident occurred in January, the VA did not begin to notify impacted physicians until months later. Furthermore, physicians were not told to report any complaints about unusual billing activity to the U.S. Department of Health and Human Services' (HHS) Office of Inspector General (OIG) until that time. While CMS has reportedly concluded that the risk of fraudulent billing to the Medicare program is not high, the agency has not acknowledged the significant and real risk of identity theft now faced by 1.3 million physicians and other health care professionals. The information supplied by CMS and lost by the VA is sufficient for an individual to assume the identity of the physicians and wreak havoc on their personal finances and subject physicians to years of time consuming and burdensome wrangling to rectify their financial standing.

In addition, the Government Accountability Office (GAO) issued a report in February 2006 concerning *Information Security*: *Department of Health and Human Services Needs to Fully Implement Its Program*. The contents of the GAO 2006 report outline the measures that should have already been in place to ensure such a breach did not occur. Subsequent GAO reports as recently as this week identify lax or inadequate security measures within HHS and CMS including: *Information Security: The Centers for Medicare & Medicaid Services Needs to Improve Controls over Key Communication Network,* August 2006; *Privacy: Lessons Learned about Data Breach Notification,* April 2007*;Information Security: Agencies Report Progress, but Sensitive Data Remain at Risk,* June 2007.

We urge CMS to amend and reissue the Dissemination Notice and identify with specificity the security policies and procedures that will be put in place and the steps that the agency will take will implement to mitigate harm, if, and when security breaches occur.

FOIA and Privacy Act Analysis Flawed

CMS has asserted that they are compelled pursuant to FOIA to disclose the specified data contained in the Dissemination Notice to the public at large. The agency's legal conclusions are—stated simply—incorrect. We would welcome the opportunity to discuss with CMS's legal counsel the underpinnings of these conclusions. The only justification offered by the agency to support the widespread disclosure of personally identifiable physician information was it is already publicly available in other forums. Accordingly, CMS staff have stated that their legal counsel advised them that they are, therefore, compelled to make it available to the general public. First, we have serious reservations that CMS can demonstrate that every physician has, in fact, made all of the personally identifiable information contained in the NPI application readily available to the public at large for any purpose. While the agency reportedly undertook a laborious survey of the types of personally identifiable information publicly available, it is not sufficient to generalize what is available and then deem an individual to have waived his or her rights simply because others have done so in their profession. Furthermore, CMS staff stated that an actual risk assessment has not been done to evaluate the potential increase in identity theft that this massive disclosure will precipitate nor was a meaningful analysis done of how the public disclosures will help facilitate the conduct of individuals intent on defrauding public and private health care payers.

Conclusion

We believe that immediate action is required to prevent a massive disclosure of personally identifiable information that is not supported by law. Furthermore, the disclosure will in all likelihood result in actual harm including widespread *identity theft, destruction of physician credit, and financial fraud.* There is sound basis in policy and law to limit the disclosure of personally identifiable physician information. We look forward to meeting with you to discuss this matter.

Sincerely,

Michael D. Maves, MD, MBA